



US010951591B1

(12) **United States Patent**
Nichani et al.

(10) **Patent No.:** **US 10,951,591 B1**
(45) **Date of Patent:** **Mar. 16, 2021**

(54) **SSL ENCRYPTION WITH REDUCED BANDWIDTH**

(71) Applicant: **Wells Fargo Bank, N.A.**, San Francisco, CA (US)

(72) Inventors: **Santosh Nichani**, Secunderabad (IN); **Ramanathan Ramanathan**, Bellevue, WA (US); **Srinivas Vengala**, Secunderabad (IN); **Sri Rajesh Rayudu**, Hyderabad (IN); **Rameshchandra Bhaskar Ketharaju**, Hyderabad (IN); **Shanmukeswara Donkada**, Hyderabad (IN)

(73) Assignee: **WELLS FARGO BANK, N.A.**, San Francisco, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 228 days.

(21) Appl. No.: **15/385,001**

(22) Filed: **Dec. 20, 2016**

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(52) **U.S. Cl.**
CPC **H04L 63/0428** (2013.01); **H04L 63/166** (2013.01); **H04L 67/10** (2013.01)

(58) **Field of Classification Search**
CPC ... H04L 63/0428; H04L 67/10; H04L 63/166; H04L 63/04; H04L 63/168; H04L 63/0823; H04L 63/123; H04L 63/104; H04L 63/06; H04L 63/20; H04L 63/18; H04L 63/0442; H04L 63/105; H04L 63/126; H04L 2209/56; G06F 21/6245; G06F 21/606; G06F 21/6254; G06F 21/64; G06F 21/6227; G06F 21/6218; G06F 21/602;

(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,223,287 B1 * 4/2001 Douglas H04L 63/0428
380/255
6,438,612 B1 * 8/2002 Ylonen H04L 63/0227
707/999.01

(Continued)

OTHER PUBLICATIONS

Song, Y., Beznosov, K. & Leung, V.C.M. , Multiple-Channel Security Architecture and its Implementation over SSL, J Wireless Com Network (2006) 2006: 085495.*

(Continued)

Primary Examiner — David Garcia Cervetti

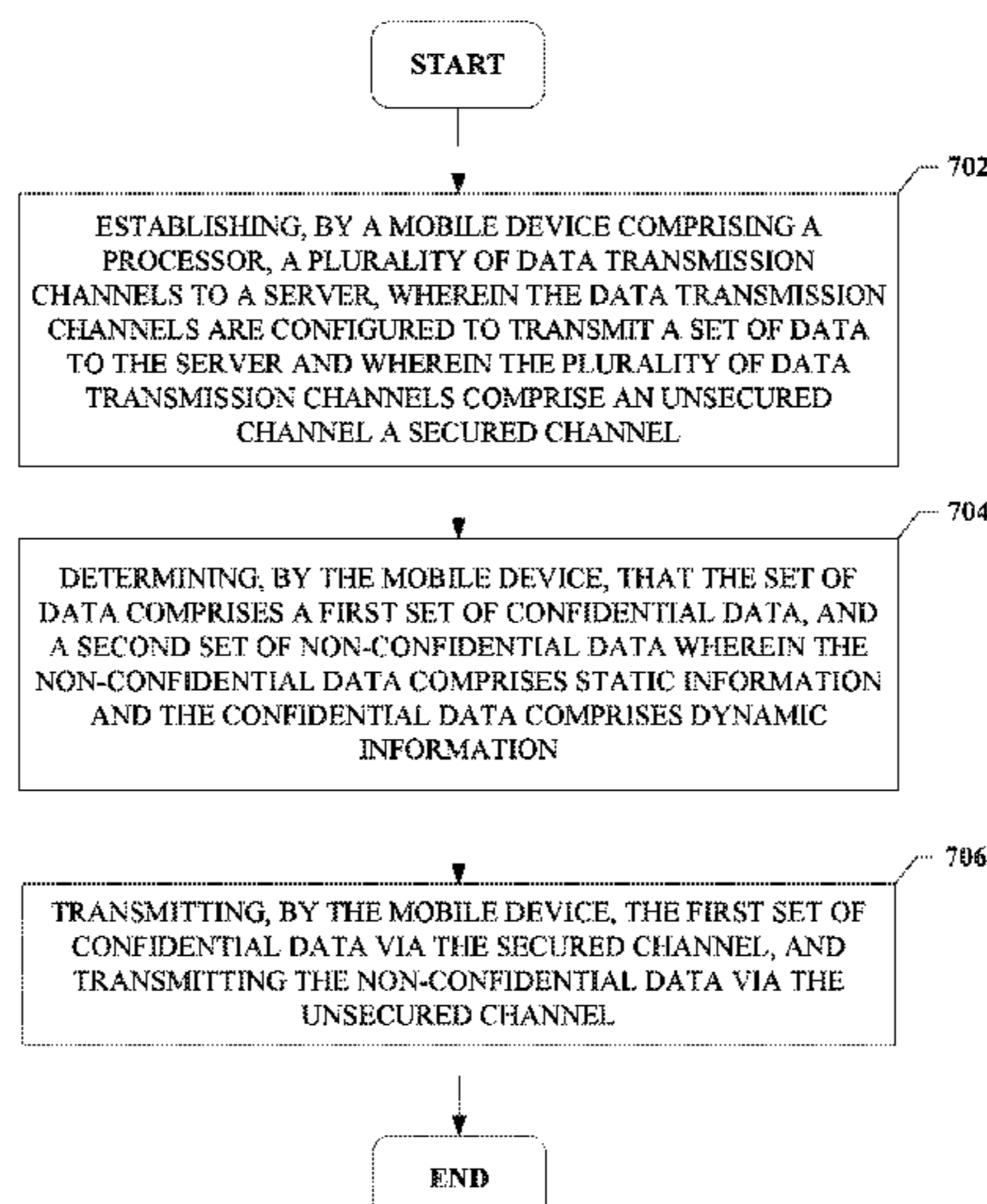
(74) *Attorney, Agent, or Firm* — Walter Haverfield LLP; James J. Pingor

(57) **ABSTRACT**

Systems and methods provide for a solution for encryption by dynamically opening multiple channels between the client and the server, where the channels include both secured (e.g., SSL/TLS and etc.) channels and non-secured channels. Non-sensitive information can be over non-secured channels, and sensitive information can be sent via the secured channels. The system can recognize whether the information is sensitive or not via the use of tags on a page or frame that delineate which information is sensitive. For instance, on a form, tags can mark off the areas of the form that may contain sensitive information, such as social security numbers, names, addresses, financial information and other private information. All the data within the tags can be considered sensitive and so be communicated to the server via a secure channel while other data can be transmitted through unsecured channels.

20 Claims, 10 Drawing Sheets

700



(58) **Field of Classification Search**
 CPC G06F 21/6263; G06F 21/6209; G06F
 21/608; G06F 3/0622; H04W 12/02
 See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,918,039 B1 *	7/2005	Hind	G06F 21/6218	713/176	2005/0086510 A1 *	4/2005	Nicodemus	H04L 63/0272	726/26
7,225,259 B2 *	5/2007	Ho	H04L 12/4633	370/230	2005/0091499 A1 *	4/2005	Forlenza	H04L 9/00	713/176
7,673,048 B1 *	3/2010	O'Toole, Jr.	H04L 12/66	709/226	2005/0132070 A1 *	6/2005	Redlich	G06F 21/6209	709/228
7,725,584 B1 *	5/2010	Hanmann	H04W 4/00	709/227	2005/0138109 A1 *	6/2005	Redlich	G06F 21/6272	709/201
7,864,686 B2 *	1/2011	Chapman	H04L 12/1859	370/237	2005/0138110 A1 *	6/2005	Redlich	G06F 21/6209	709/201
8,068,499 B2	11/2011	Vidya et al.				2005/0235163 A1 *	10/2005	Forlenza	G06F 21/6209	713/193
8,364,980 B2 *	1/2013	Forlenza	G06F 21/62	713/189	2005/0235165 A1 *	10/2005	Gomez	G06F 16/9577	713/193
8,418,244 B2	4/2013	Sinn				2005/0246526 A1 *	11/2005	Forlenza	H04L 9/088	713/165
8,542,823 B1 *	9/2013	Nguyen	G06F 21/602	380/42	2005/0262418 A1 *	11/2005	Gehrmann	H04L 9/3033	714/758
8,561,127 B1	10/2013	Agrawal et al.				2005/0273841 A1 *	12/2005	Freund	H04L 63/102	726/1
8,688,978 B2 *	4/2014	Struik	H04L 63/105	713/160	2006/0050879 A1 *	3/2006	Iizuka	G06F 21/608	380/51
8,745,379 B2	6/2014	Orsini et al.				2006/0050883 A1 *	3/2006	Walker	H04N 21/4367	380/239
8,775,823 B2 *	7/2014	Gokhale	G06F 21/78	713/189	2006/0053441 A1 *	3/2006	Walker	H04K 1/00	725/30
8,776,249 B1 *	7/2014	Margolin	G06F 21/6209	726/26	2006/0069917 A1 *	3/2006	Martin	H04L 63/0823	713/175
8,856,869 B1 *	10/2014	Brinskelle	G06F 21/6218	726/2	2006/0075228 A1 *	4/2006	Black	H04L 63/104	713/167
8,856,910 B1 *	10/2014	Rostami-Hesarsorkh	G06F 21/554	726/11	2006/0143459 A1 *	6/2006	Villaron	G06F 21/6254	713/176
8,938,611 B1 *	1/2015	Zhu	G06F 21/575	713/153	2006/0195547 A1 *	8/2006	Sundarrajan	H04L 69/163	709/217
9,088,550 B1 *	7/2015	Taraki	H04N 21/8549		2006/0200849 A1 *	9/2006	Sundarrajan	H04L 69/163	725/110
9,137,262 B2	9/2015	Qureshi et al.				2006/0277406 A1 *	12/2006	Hashimoto	H04L 63/029	713/168
9,183,380 B2	11/2015	Qureshi et al.				2007/0076882 A1 *	4/2007	Engel	H04L 63/0457	380/255
9,185,033 B2 *	11/2015	Khalid	H04L 43/0829		2007/0094373 A1 *	4/2007	Brendel	H04L 63/166	709/223
9,218,500 B2 *	12/2015	Eldar	G06F 21/6218		2007/0180134 A1 *	8/2007	Steinbach	H04L 41/083	709/230
9,223,995 B1 *	12/2015	Lavinio	H04L 63/0421		2007/0195960 A1 *	8/2007	Goldman	H04L 9/30	380/286
9,304,716 B2 *	4/2016	Takasu	G06F 3/1238		2007/0206738 A1 *	9/2007	Patel	H04M 3/53333	379/93.24
9,325,742 B1 *	4/2016	Barsness	H04L 63/20		2008/0040776 A1 *	2/2008	Bauer	G06F 21/602	726/3
9,521,118 B2 *	12/2016	Cottrell	H04L 67/28		2008/0131861 A1 *	6/2008	Redd	G09B 7/00	434/362
9,690,763 B1 *	6/2017	Lee	G06F 16/954		2008/0133915 A1 *	6/2008	Tanaka	H04L 63/029	713/171
9,923,923 B1 *	3/2018	Sharifi Mehr	H04L 9/14		2009/0028049 A1 *	1/2009	Boudreau	H04L 51/38	370/235
10,068,099 B1 *	9/2018	Fishbeck	G06F 21/6218		2009/0119504 A1 *	5/2009	van Os	H04L 9/3271	713/153
10,116,591 B2 *	10/2018	Sung	H04L 45/74		2009/0204711 A1 *	8/2009	Binyamin	H04L 67/1021	709/226
10,133,873 B2 *	11/2018	Kritt	G06F 21/6209		2009/0222927 A1 *	9/2009	Pikus	G06F 30/398	726/26
10,225,075 B1 *	3/2019	Moritz	H04L 9/0625		2009/0224884 A1 *	9/2009	Tuttle	H04W 12/0013	340/10.1
10,243,990 B1 *	3/2019	Chen	G06F 21/71		2009/0253511 A9 *	10/2009	Loose	A63F 13/71	463/42
10,255,445 B1 *	4/2019	Brinskelle	H04L 63/0428		2009/0254572 A1 *	10/2009	Redlich	G06Q 10/06	
2002/0025045 A1 *	2/2002	Raike	H04L 63/0457	380/280	2010/0030839 A1 *	2/2010	Ceragioli	H04L 67/1036	709/201
2002/0112167 A1 *	8/2002	Boneh	H04L 63/0428	713/182	2010/0146600 A1 *	6/2010	Eldar	G06F 21/6218	726/5
2003/0159030 A1 *	8/2003	Evans	H04L 29/06	713/154	2010/0162348 A1 *	6/2010	Narayanan	H04L 63/105	726/1
2003/0182576 A1 *	9/2003	Morlang	H04L 69/24	713/171	2010/0211792 A1 *	8/2010	Ureche	H04L 63/102	713/176
2004/0034776 A1 *	2/2004	Fernando	H04L 9/321	713/171						
2004/0078596 A1 *	4/2004	Kent, Jr.	H04L 63/0457	713/160						
2004/0162076 A1 *	8/2004	Chowdry	H04L 67/16	455/445						
2004/0172476 A1 *	9/2004	Chapweske	H04L 67/325	709/231						
2005/0071792 A1 *	3/2005	Ferguson	G06F 21/6209	716/102						

(56)

References Cited

U.S. PATENT DOCUMENTS

2010/0250497 A1* 9/2010 Redlich H04L 63/0227
707/661
2010/0250944 A1* 9/2010 Suzuki H04L 63/0861
713/172
2010/0299529 A1* 11/2010 Fielder G06F 21/602
713/181
2010/0299744 A1* 11/2010 Mardiks G06F 21/10
726/17
2010/0325421 A1* 12/2010 Park H04L 9/0825
713/153
2010/0325717 A1* 12/2010 Goel H04L 63/102
726/11
2011/0072507 A1* 3/2011 Johnston, II H04L 63/0853
726/12
2011/0085666 A1* 4/2011 Hicks H04L 9/0852
380/278
2011/0131640 A1* 6/2011 Canis Robles G06F 21/606
726/7
2011/0154443 A1* 6/2011 Thakur G06F 21/41
726/3
2011/0307706 A1* 12/2011 Fielder H04L 9/3228
713/181
2012/0023158 A1* 1/2012 Kashyap H04L 63/0428
709/203
2012/0150747 A1* 6/2012 Carey H04L 9/0827
705/71
2012/0182884 A1* 7/2012 Pyatkovskiy H04L 63/166
370/250
2012/0284513 A1* 11/2012 Yerli H04L 67/38
713/168
2012/0290837 A1* 11/2012 Vion-Dury H04L 9/14
713/167
2012/0304246 A1* 11/2012 Zhang H04W 12/02
726/1
2012/0326847 A1 12/2012 Strauman
2013/0036313 A1* 2/2013 Schwenk H04L 63/0428
713/193
2013/0047264 A1* 2/2013 Bjorkengren G06F 21/105
726/27
2013/0167192 A1* 6/2013 Hickman G06F 21/60
726/1
2013/0336482 A1* 12/2013 Waisbard H04N 21/4623
380/210
2014/0115328 A1* 4/2014 Allen H04L 29/06
713/165
2014/0129661 A1* 5/2014 Thyagaraja H04L 51/24
709/207
2014/0240753 A1* 8/2014 Anno G06F 3/1206
358/1.15
2014/0297440 A1* 10/2014 Fredell G06Q 20/3278
705/21
2014/0301204 A1* 10/2014 Koshimizu H04W 28/0289
370/235
2014/0325236 A1* 10/2014 Kim G06F 21/62
713/189
2014/0337614 A1* 11/2014 Kelson H04L 63/20
713/152
2014/0351920 A1 11/2014 Madani
2014/0366084 A1* 12/2014 Ogawa G06F 21/57
726/1

2015/0043730 A1* 2/2015 Thompson H04L 63/0272
380/42
2015/0082022 A1* 3/2015 Marinkovic G06Q 20/3829
713/153
2015/0119017 A1* 4/2015 Wu H04W 8/245
455/419
2015/0128204 A1* 5/2015 Lietz H04L 63/0428
726/1
2015/0188949 A1* 7/2015 Mahaffey H04W 12/0027
726/1
2015/0215899 A1* 7/2015 Kumar H04W 12/08
455/59
2015/0229614 A1* 8/2015 Thompson H04L 63/029
713/168
2015/0263859 A1* 9/2015 Lietz H04L 69/18
713/168
2015/0271163 A1* 9/2015 Greenspan H04L 63/18
713/168
2015/0347770 A1* 12/2015 Whalley G06F 21/6245
726/30
2015/0350247 A1* 12/2015 Adler H04L 63/061
713/151
2015/0381578 A1* 12/2015 Thota H04L 63/1408
713/168
2015/0382240 A1* 12/2015 Hecht H04L 69/18
370/316
2016/0094467 A1* 3/2016 Hong H04L 63/0281
370/235
2016/0112195 A1* 4/2016 Jochheim H04L 9/0816
713/189
2016/0182466 A1* 6/2016 Wagenaar H04L 63/0464
713/154
2016/0224800 A1* 8/2016 Bellert G06F 21/6245
2016/0239668 A1* 8/2016 Bellert G06F 21/602
2016/0275303 A1* 9/2016 Narayanaswamy .. H04L 9/0861
2016/0315762 A1* 10/2016 Moon H04L 9/065
2016/0323818 A1* 11/2016 Senarath H04W 52/0277
2017/0063933 A1* 3/2017 Shieh H04L 63/107
2017/0083717 A1* 3/2017 Medvedev H04L 63/1416
2017/0099144 A1* 4/2017 Sobel H04L 63/083
2017/0156172 A1* 6/2017 Yokoyama H04W 68/12
2017/0180155 A1* 6/2017 Shanks H04L 12/4633
2017/0181128 A1* 6/2017 Zhu H04L 9/065
2017/0201495 A1* 7/2017 Cooley G06Q 20/108
2017/0213041 A1* 7/2017 Medvedev H04L 63/0428
2017/0264619 A1* 9/2017 Narayanaswamy
G06F 21/6209
2017/0337383 A1* 11/2017 Eldar G06F 9/44521
2017/0353745 A1* 12/2017 Karkkainen H04N 21/23476
2018/0025180 A1* 1/2018 Wang G06F 21/6281
726/1
2018/0157853 A1* 6/2018 Kumar G06F 12/1408
2018/0183608 A1* 6/2018 Koyun H04L 63/0428
2018/0196761 A1* 7/2018 Rieken H04L 63/061
2018/0205743 A1* 7/2018 McIver H04L 63/0428

OTHER PUBLICATIONS

WolfSSL State of the Art Networking Security for Embedded Systems; <http://www.freertos.org/FreeRTOS-Plus/WolfSSL/WolfSSL.shtml>; pp. 1-4; 2010-2016 Real Time Engineers Ltd.

* cited by examiner

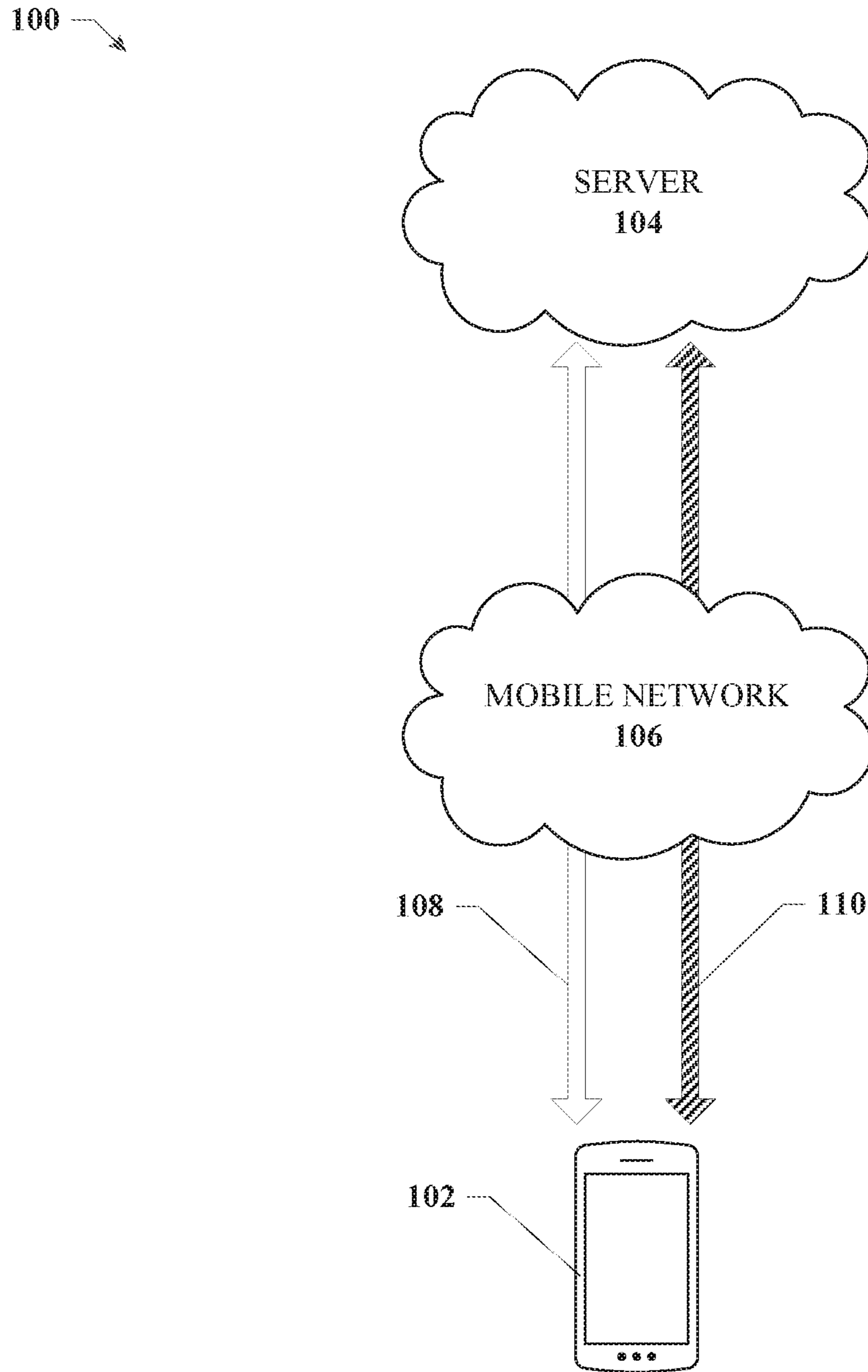


FIG. 1

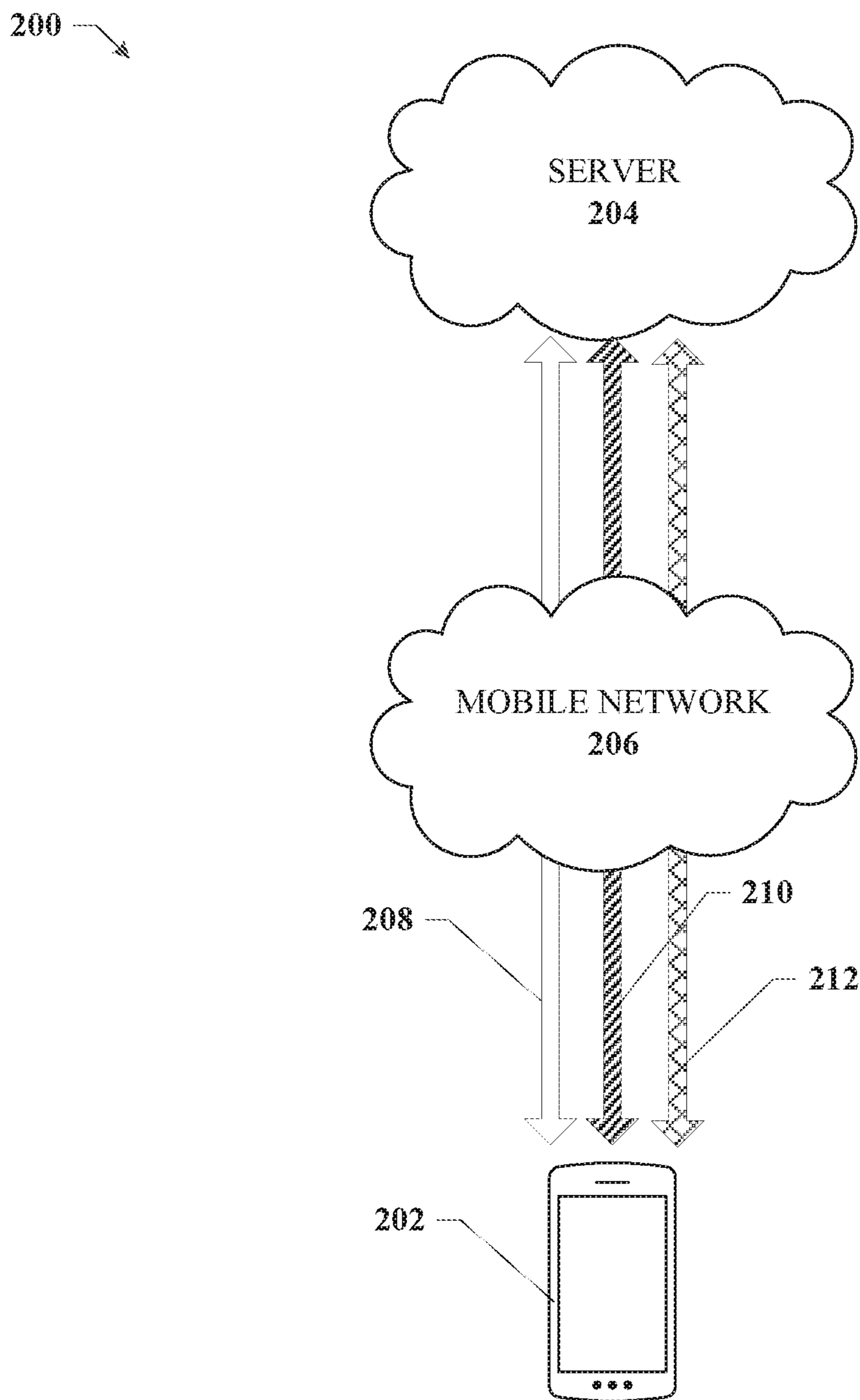


FIG. 2

300 ↘

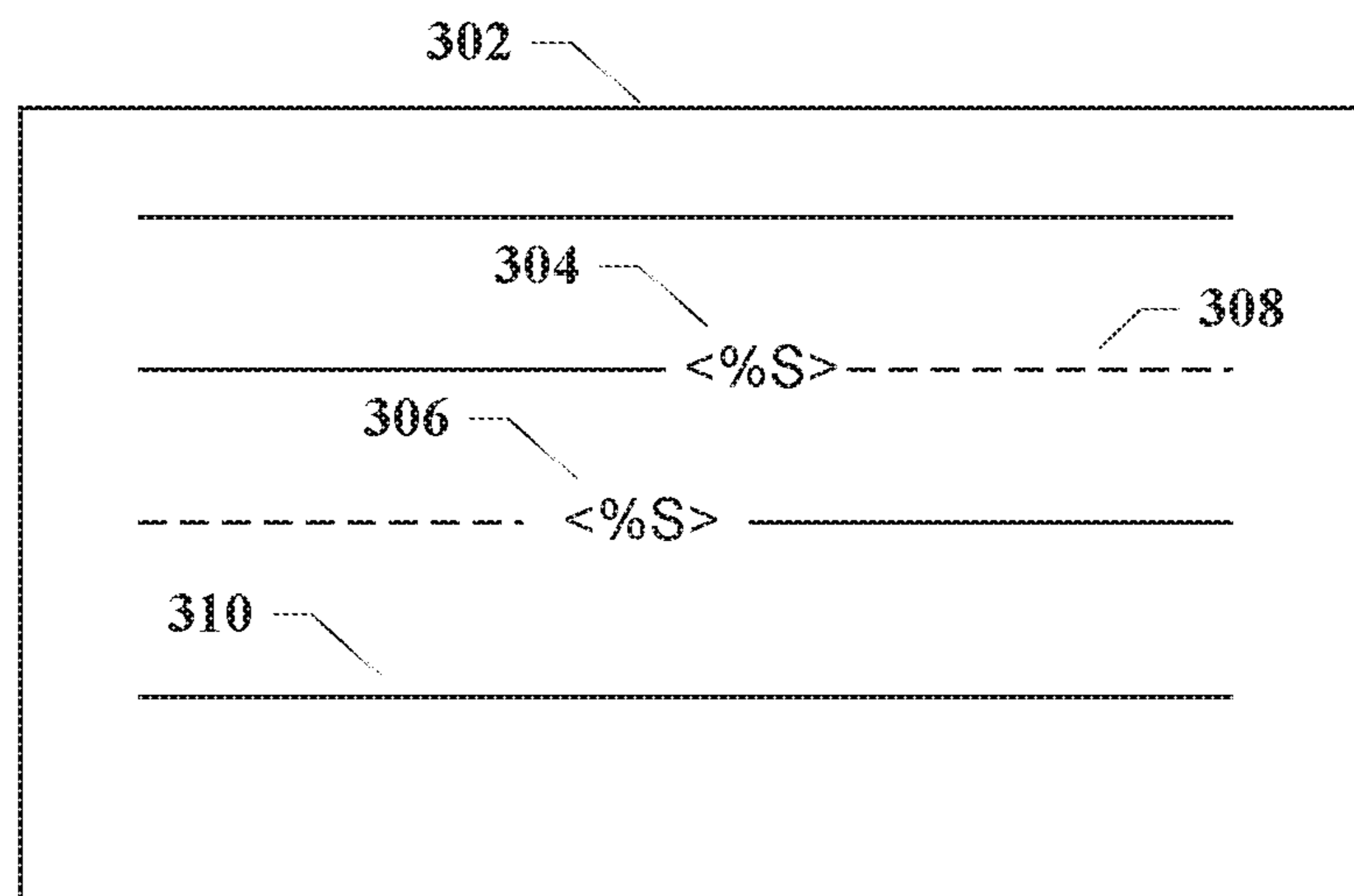


FIG. 3

400 ↘

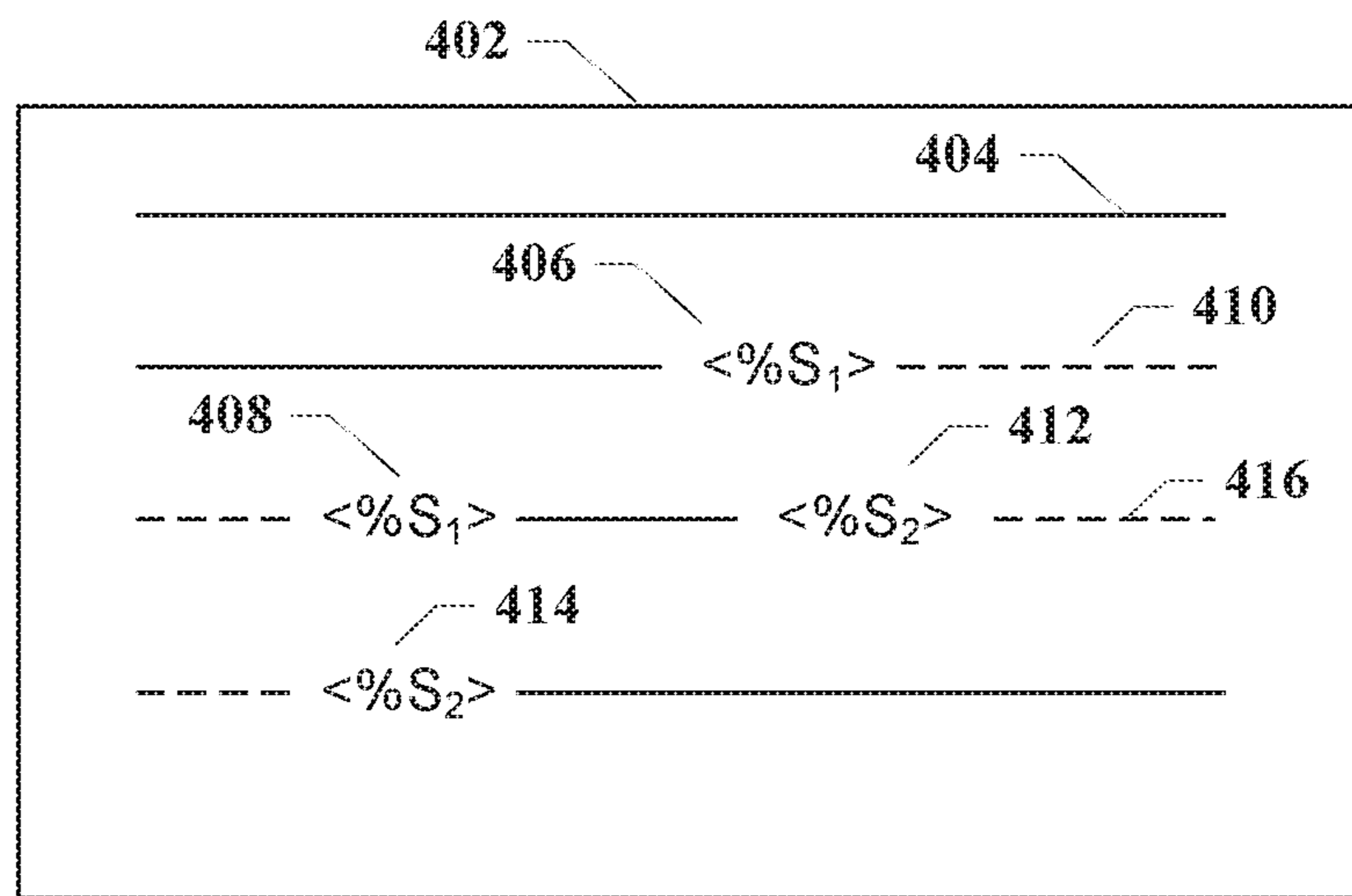


FIG. 4

500 ↘

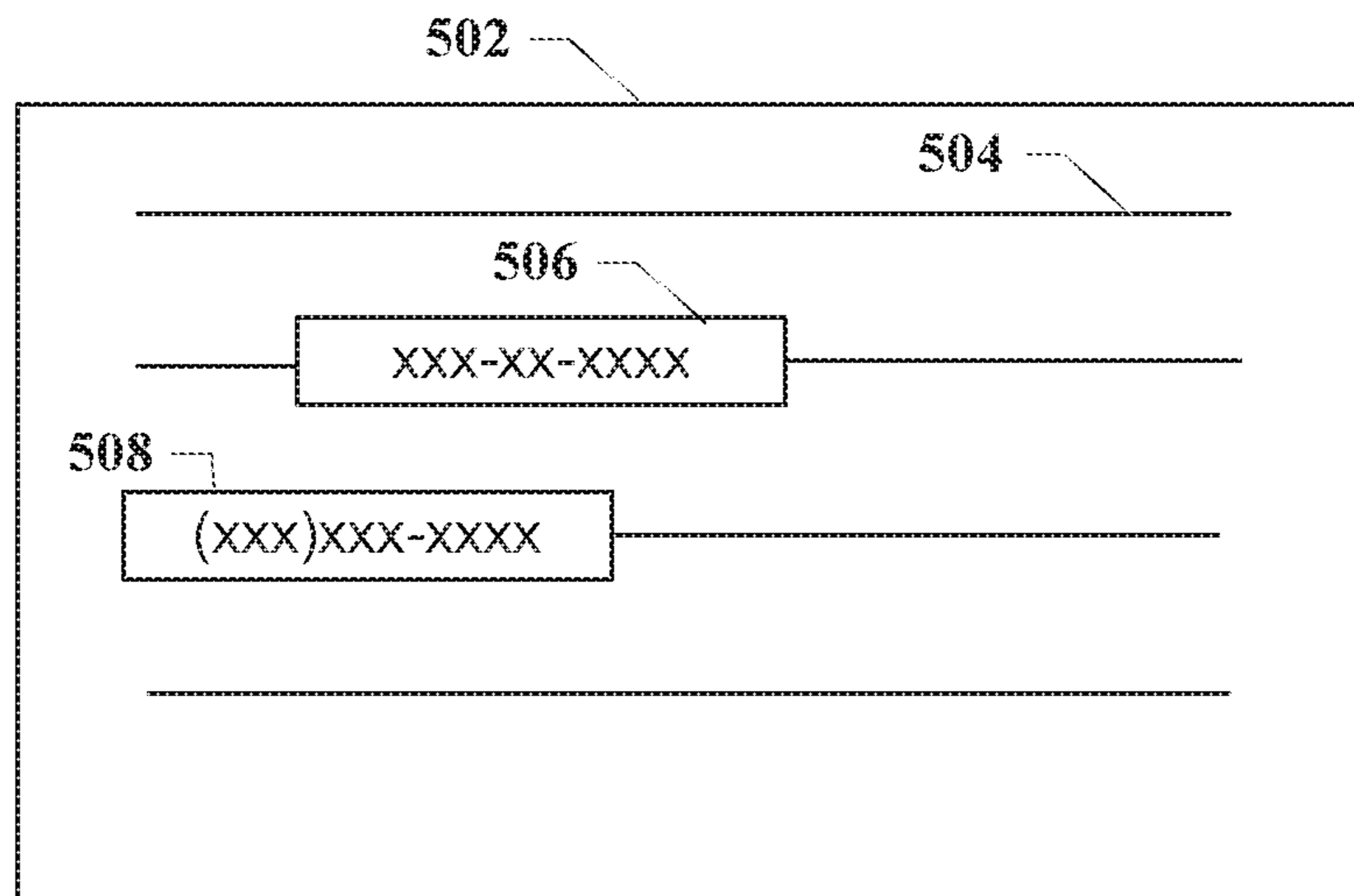


FIG. 5

600 →

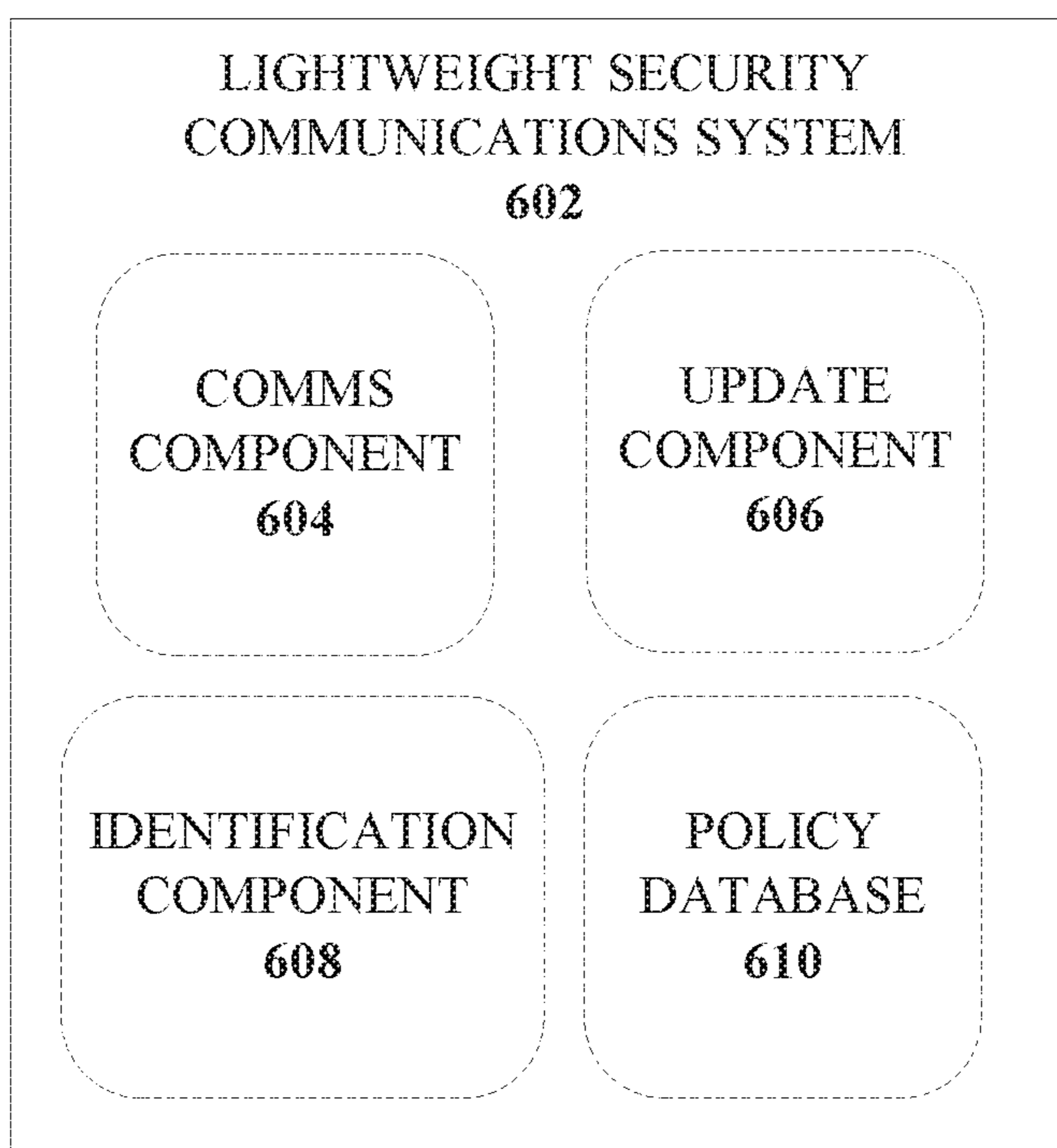


FIG. 6

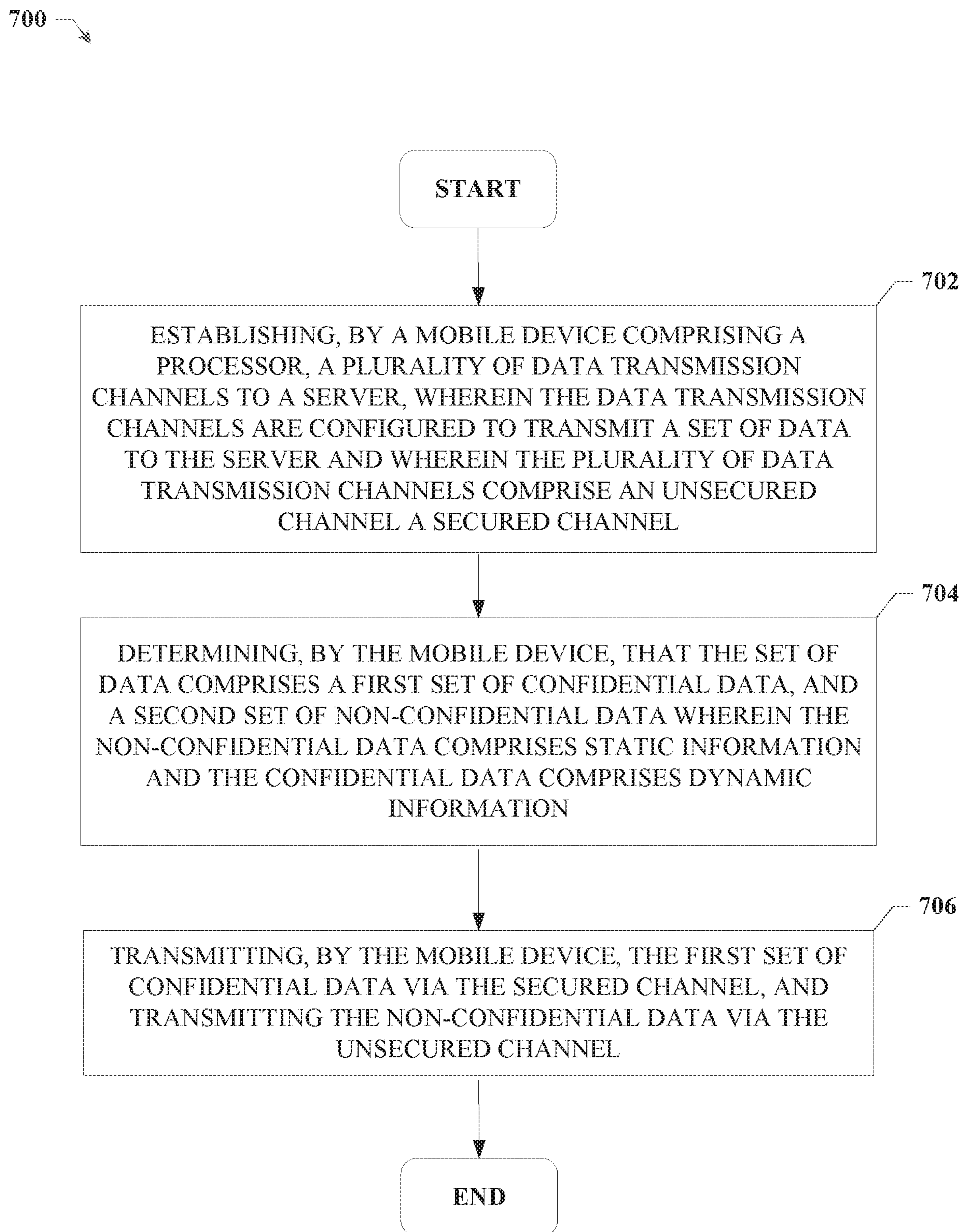


FIG. 7

800

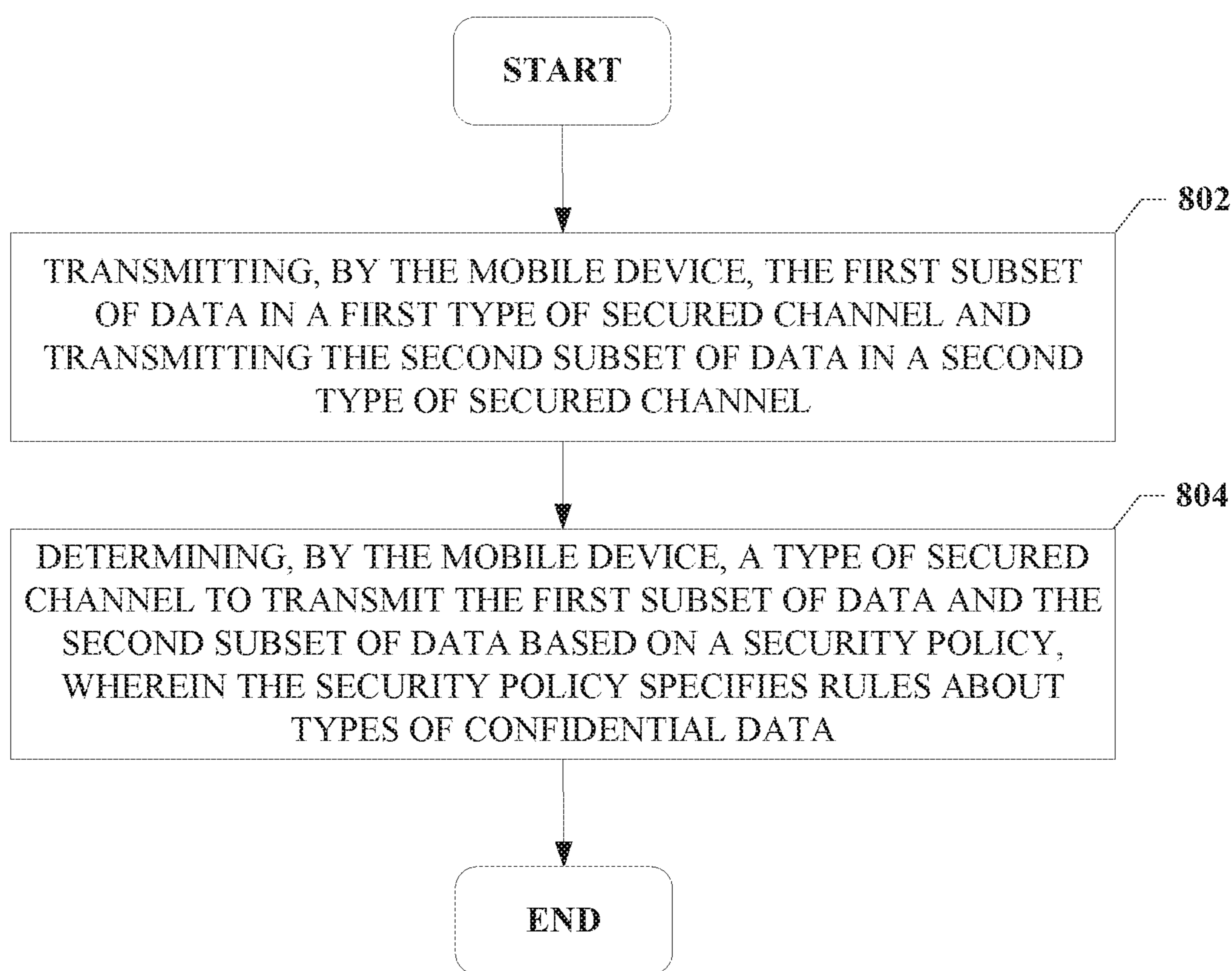


FIG. 8

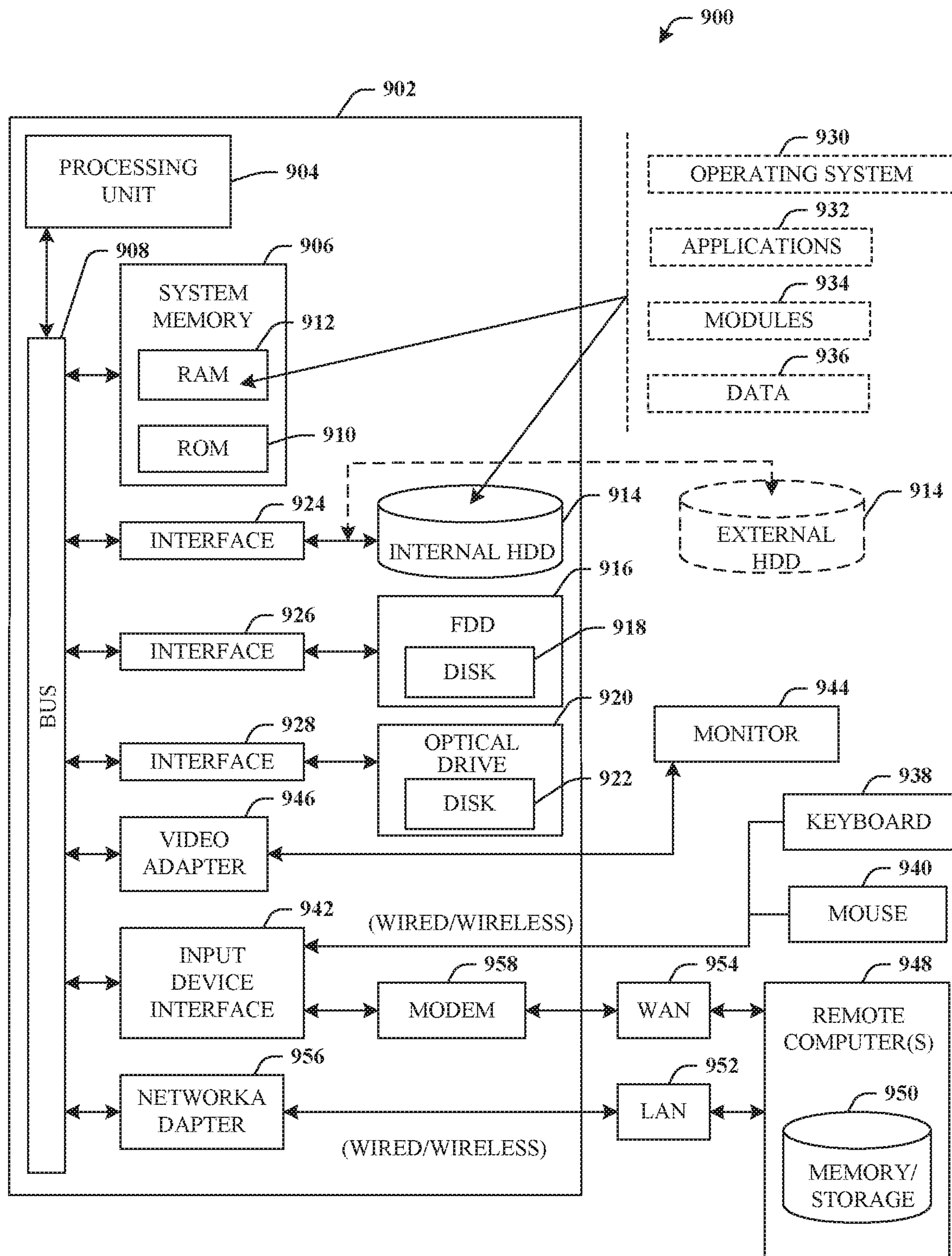


FIG. 9

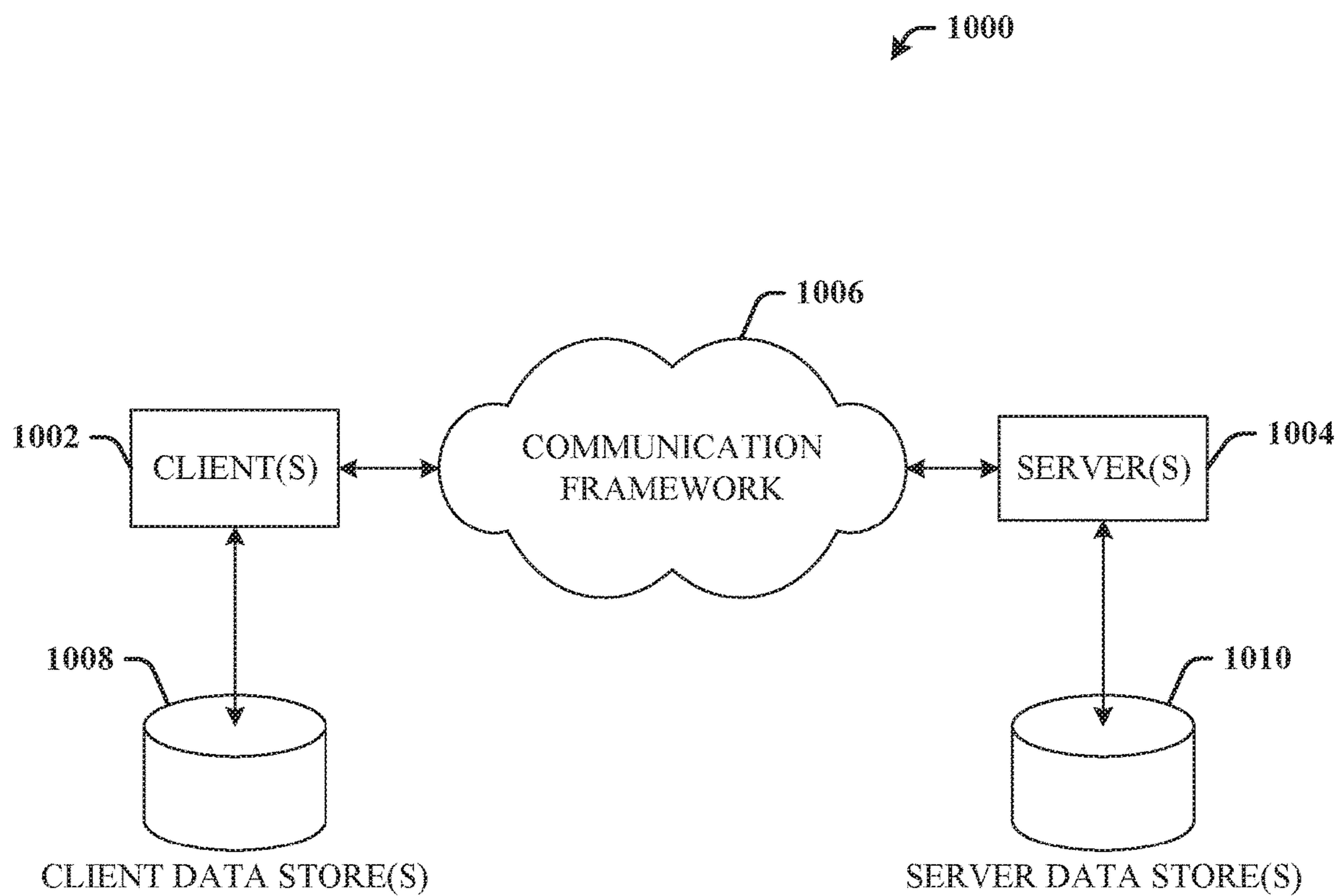


FIG. 10

SSL ENCRYPTION WITH REDUCED BANDWIDTH

BACKGROUND

Secure Sockets Layer (SSL) and Transport Layer Security (TLS—also often referred to as SSL) are security technologies for establishing an encrypted link between a web server and a browser. These links ensure that data passed between the web server and the browsers remains private and integral. However, SSL and TLS layers impact the communications performance. During the handshake protocol the secure link is established between the client and the server with an asymmetric cipher to establish cipher settings and a shared key for a session are exchanged. This handshake is computationally intense however, and consumes a significant amount of a processor resources, especially for light-weight mobile devices and Internet of Things (IoT) devices.

SUMMARY

The following presents a simplified summary in order to provide a basic understanding of some aspects of the innovation. This summary is not an extensive overview of the innovation. It is not intended to identify key/critical elements or to delineate the scope of the innovation. Its sole purpose is to present some concepts of the innovation in a simplified form as a prelude to the more detailed description that is presented later.

The disclosure disclosed and claimed herein, in one aspect thereof, includes systems and methods that facilitate a solution for encryption by dynamically opening multiple channels between the client and the server, where the channels include both secured (e.g., SSL/TLS and etc.) channels and non-secured channels. Non-sensitive information can be communicated over non-secured channels, and sensitive information can be sent via the secured channels. The system can recognize whether the information is sensitive or not via the use of tags on a page or frame that delineate which information is sensitive. For instance, on a form, tags can mark off the areas of the form that may contain sensitive information, such as social security numbers, names, addresses, financial information and other private information. All the data within the tags can be considered sensitive and be communicated to the server via a secure channel. All other information, including page layout, style, and template information can be sent over unsecured channels that do not require the same computing power as the secured channels.

It is to be appreciated that, in aspects, tags can be used to determine and/or establish what type of security policy should be used. Some require strong encryption, some might not need encryption at all, and some might require 'light weight' encryption. If there are no tags then the information will be transmitted in clear-text. If there is a tag then the information between the beginning of the tag to the end of tag will be sent according to the security policy of the tag. As will be understood, there can be 'n' number of tags in a document collectively represent 'm' security policies ($m \leq n$). The computer will scan the document before sending and determine the number of channels to open based on the type of tags present. In other embodiments, the system can also do that at run time without prescanning. It can start with one non-secure channel (e.g., clear-text channel) and as it encounters a tag it can determine whether it has to open a new secure channel or not.

For these considerations, as well as other considerations, in one or more embodiments, a system can include a memory to store computer-executable instructions and a processor, coupled to the memory, to facilitate execution of the computer-executable instructions to perform operations. The operations can include establishing a plurality of data transmission channels to a server, wherein the data transmission channels are configured to transmit a set of data to the server and wherein the plurality of data transmission channels comprise an unsecured channel a secured channel. The operations can also include determining that the set of data comprises a first set of confidential data, and a second set of non-confidential data. The operations can also include transmitting the first set of confidential data via the secured channel, and transmitting the non-confidential data via the unsecured channel.

In another embodiment, a method for providing secured communications can include establishing, by a mobile device comprising a processor, a plurality of data transmission channels to a server, wherein the data transmission channels are configured to transmit a set of data to the server and wherein the plurality of data transmission channels comprise an unsecured channel a secured channel. The method can also include determining, by the mobile device, that the set of data comprises a first set of confidential data, and a second set of non-confidential data wherein the non-confidential data comprises static information and the confidential data comprises dynamic information. The method can also include transmitting, by the mobile device, the first set of confidential data via the secured channel, and transmitting the non-confidential data via the unsecured channel.

In another embodiment, a non-transitory computer-readable medium can comprise instructions that when executed by a computer processor perform operations including establishing a plurality of data transmission channels to a server, wherein the data transmission channels are configured to transmit a set of data to the server and wherein the plurality of data transmission channels comprise an unsecured channel a secured channel. The operations can also include determining that the set of data comprises a first set of confidential data, and a second set of non-confidential data wherein the first set of confidential data comprise a first subset of a first type of confidential data and a second subset of a second type of confidential data. The operations can further include transmitting the first set of confidential data via the secured channel, and transmitting the non-confidential data via the unsecured channel.

To accomplish the foregoing and related ends, certain illustrative aspects of the innovation are described herein in connection with the following description and the annexed drawings. These aspects are indicative, however, of but a few of the various ways in which the principles of the innovation can be employed and the subject innovation is intended to include all such aspects and their equivalents. Other advantages and novel features of the innovation will become apparent from the following detailed description of the innovation when considered in conjunction with the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an illustration of an example system for providing a SSL/TLS encryption system in accordance with one or more aspects of the disclosure.

FIG. 2 is an illustration of an example system for providing a SSL/TLS encryption system with multiple secure channels in accordance with one or more aspects of the disclosure.

FIG. 3 is an illustration of an example system for providing a SSL/TLS encryption system that uses tags in accordance with one or more aspects of the disclosure.

FIG. 4 is an illustration of an example system for providing a SSL/TLS encryption system that uses tags for multiple types of secure channels in accordance with one or more aspects of the disclosure.

FIG. 5 is an illustration of an example system for providing a SSL/TLS encryption system that can identify sensitive information in accordance with one or more aspects of the disclosure.

FIG. 6 is an illustration of an example system for providing a SSL/TLS encryption system in accordance with one or more aspects of the disclosure.

FIG. 7 is an illustration of an example flow chart of a method for providing encryption according to one or more embodiments.

FIG. 8 is an illustration of an example flow chart of a method for providing encryption according to one or more embodiments.

FIG. 9 is an illustration of an example computing environment where one or more of the provisions set forth herein are implemented, according to one or more embodiments.

FIG. 10 is an illustration of an example computing environment where one or more of the provisions set forth herein are implemented, according to one or more embodiments.

DETAILED DESCRIPTION

The following terms are used throughout the description, the definitions of which are provided herein to assist in understanding various aspects of the disclosure.

As used in this disclosure, the term “device” or “client device” refers to devices, items or elements that may exist in an organization’s network, for example, users, groups of users, computer, tablet computer, smart phone, iPad®, iPhone®, wireless access point, wireless client, thin client, applications, services, files, distribution lists, resources, printer, fax machine, copier, scanner, multi-function device, mobile device, badge reader and most any other networked element.

The innovation is now described with reference to the drawings, wherein like reference numerals are used to refer to like elements throughout. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the subject innovation. It may be evident, however, that the innovation can be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to facilitate describing the innovation.

While specific characteristics are described herein, it is to be understood that the features, functions and benefits of the innovation can employ characteristics that vary from those described herein. These alternatives are to be included within the scope of the innovation and claims appended hereto.

While, for purposes of simplicity of explanation, the one or more methodologies shown herein, e.g., in the form of a flow chart, are shown and described as a series of acts, it is to be understood and appreciated that the subject innovation is not limited by the order of acts, as some acts may, in

accordance with the innovation, occur in a different order and/or concurrently with other acts from that shown and described herein. For example, those skilled in the art will understand and appreciate that a methodology could alternatively be represented as a series of interrelated states or events, such as in a state diagram. Moreover, not all illustrated acts may be required to implement a methodology in accordance with the innovation.

As used in this application, the terms “component” and “system” are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution. For example, a component can be, but is not limited to being, a process running on a processor, a processor, an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a server and the server can be a component. One or more components can reside within a process and/or thread of execution, and a component can be localized on one computer and/or distributed between two or more computers.

In one or more embodiments a solution for encryption can be provided by dynamically opening multiple channels between the client and the server, where the channels include both secured (e.g., SSL/TLS and etc.) channels and non-secured channels. Non-sensitive information can be over non-secured channels, and sensitive information can be sent via the secured channels.

The system can recognize whether the information is sensitive or not via the use of tags on a page or frame that delineate which information is sensitive. For instance, on a form, tags can mark off the areas of the form that may contain sensitive information, such as social security numbers, names, addresses, financial information and other private information. All the data within the tags can be considered sensitive and so be communicated to the server via a secure channel. All other information, including page layout, style, and template information can be sent over unsecured channels that don’t require the same computing power as the secured channels.

In an embodiment, the dynamic information can be sent over the secured channels while static information can be sent over unsecured channels. In other embodiments, the system can determine whether information is sensitive or not based on an analysis of the data and determining character types, formats, and length. For instance, credit card numbers can be identified based on a recognizable sequence of numbers, while social security numbers and other identification numbers can be based on identifying sequences of numbers (e.g., xxx-xx-xxxx).

In an embodiment, the tags that are used to identify sensitive information can be further separated into different types of tags based on the field or type of information. For instance, Tag A can refer to a certain type of sensitive data, Tag B can refer to a second type of sensitive data and so forth. The system can refer to a security policy for the client or server or site in order to determine how to treat various types of information or types of tags. For instance, Tag A can have a first security policy assigned, while Tag B can have a second security policy. The security policies can include rules about which types of encryption are used, who is authorized to access the data, and other security rules.

Turning now to FIG. 1, illustrated is an example system 100 for providing a SSL/TLS encryption system in accordance with one or more aspects of the disclosure. The system 100 in FIG. 1 includes a mobile device 102 that can send and receive data to and from a server 104 via a mobile network 106. To protect sensitive information such as name, address,

phone number, financial information and other identifying information, the mobile device **102** and server **104** can establish a secured link that uses encryption to protect the information contained in the communications.

In traditional communications, the server **104** and the mobile device **102** would establish a secure channel and all of the data passed between the server **104** and the mobile device **102** would pass through the secure channel. In the embodiment disclosed herein however, the mobile device **102** can simultaneously establish a first channel **108** that is unsecured, and a second channel **110** that is secured. Unsecured channel **108** can facilitate transmission of unsecured data or data that is not sensitive, while secured channel **110** can facilitate transmission of secured or sensitive data.

By way of example, if mobile device **102** was transmitting form information from a website, the content of the forms may be sensitive and so that data can be transmitted to the server **104** via the mobile network **106** by the secured channel **110**. Other information transmitted, such as the layout, template, style data, etc, can be transmitted by the unsecured channel **108**. Since data transmitted by the secured channel **110** requires greater computer processing resources to encrypt, by reducing the amount of data sent via the secured channel **110**, and by sending it via an unsecured channel **108**, the computing resources required by mobile device **102** can be decreased, improving battery life, reducing the processing requirements, and improving bandwidth of the mobile device **102**.

The mobile device **102** and/or the server **104** can determine what is sensitive data or data that otherwise should be encrypted in a variety of ways. In one embodiment, data can be tagged using metadata or HTML tags or other forms of tags, where the tagged data is data the intended to be secured via SSL encryption. In an embodiment, the mobile device **102** or server **104**, depending on whether the data is being transmitted to the server **104** or to the mobile device **102** respectively, can identify the tags, and send untagged data via the unsecured channel **108** and send tagged data via the secured channel **110**.

In other embodiments, the sensitive data can be identified without the use of tags. Data that is static (e.g., the form templates, styles, outlines, etc) can be determined to be unresponsive and thus can be sent via the unsecured channel **108**. Data that is dynamic, and changes between frames, sessions, etc, can be determined to be sensitive, and thus can be sent via the secured channel **110**.

In other embodiments, the sensitive data can be identified based on a pattern analysis of the data. Commonly transmitted data that might be sensitive and thus require encryption can be financial information such as bank account numbers, routing numbers, credit card numbers, and etc. The information can also include addresses, names, birthdates, and etc. These types of information commonly follow similar formats such as a pattern of numbers and characters, length of string of characters, and etc. For instance, social security numbers can be recognized by their familiar pattern of 9 numbers separated by dashes in groups of 3, 2, and 4. Similarly, credit card numbers will have common patterns and dates will have similar patterns and other identification numbers and information can be identified similarly.

In an embodiment, the type of encryption or type of secure channel established by the mobile device **102** or server **104** can be selected based on one or more security policies located at either the client or server side. The security policy can state that a certain type of encryption should be used whenever sensitive data is identified. In other embodiments, different encryption and security schemes can

be used for different types of data. For instance, identifying data such as names and addresses can be associated with a first type of encryption scheme, while financial information can be associated with a second type of encryption scheme.

In an embodiment, separate secured channels can be opened simultaneously between server **104** and the mobile device **102** in order to transmit the different types of confidential data at the same time. The security policy can be stored in a rules database on either the mobile device **102** or the server **104**, and can specify different rules and procedures about how data is to be handled.

It is to be appreciated the secure tunnel **110** can include either SSL or TLS encryption or any other encryption scheme that a person having ordinary skill in the art would contemplate.

Turning now to FIG. 2, illustrated is an example system **200** for providing a SSL/TLS encryption system with multiple secure channels in accordance with one or more aspects of the disclosure.

The system **200** in FIG. 2 includes a mobile device **202** that can send and receive data to and from a server **204** via a mobile network **206**. To protect sensitive information such as name, address, phone number, financial information and other identifying information, the mobile device **202** and server **204** can establish a plurality of secured links **210** and **212** that use encryption to protect the information contained in the communications.

In an embodiment, the type of encryption or type of secure channel established by the mobile device **202** or server **204** can be selected based on one or more security policies located at either the client or server side. The security policy can state that a certain type of encryption should be used whenever sensitive data is identified. In other embodiments, different encryption and security schemes can be used for different types of data. For instance, identifying data such as names and addresses can be associated with a first type of encryption scheme, while financial information can be associated with a second type of encryption scheme. In an embodiment, separate secured channels (e.g. **210** and **212**) can be opened simultaneously between server **204** and the mobile device **202** in order to transmit the different types of confidential data at the same time. The security policy can be stored in a rules database on either the mobile device **202** or the server **204**, and can specify different rules and procedures about how data is to be handled.

The mobile device **202** and/or the server **204** can determine what type of sensitive data is present and determine whether it should be transmitted by secure channel **210**, or secure channel **212**, or by unsecured channel **208**. In one embodiment, data can be tagged using metadata or HTML tags or other forms of tags, where the tagged data is data the intended to be secured via SSL encryption. The tag can include information identifying the type of confidential data, or include information identifying the type of encryption required. In an embodiment, the mobile device **202** or server **204**, depending on whether the data is being transmitted to the server **204** or to the mobile device **202** respectively, can identify the tags, and send untagged data via the unsecured channel **208** and send tagged data via either the secured channel **210** or secured channel **212**.

In other embodiments, the sensitive data can be identified without the use of tags. Data that is static (e.g., the form templates, styles, outlines, etc) can be determined to be unresponsive and thus can be sent via the unsecured channel **208**. Data that is dynamic, and changes between frames, sessions, etc, can be determined to be sensitive, and thus can

be sent via either the secured channel **210** or the secured channel **212** based on the type of data identified.

In some embodiments, the type secured channels created can be based on the time of transmission or based on the location of the mobile device. For instance, if the mobile device **202** is in a location known to have less secure mobile networks (e.g., mobile network **206**), the rules can specify a higher level of encryption or different type of encryption (256 bit instead of 128 bit, and etc).

Turning now to FIG. **3**, illustrated is an example system **300** for providing a SSL/TLS encryption system that uses tags in accordance with one or more aspects of the disclosure. In an embodiment, a set of data **302** can include data **310** that does not require encryption, and can be sent via an unsecured channel. The set of data **302** can also include sensitive data **308** that is identified based on an opening tag **304** and a closing tag **306**. These tags can indicate to the mobile device that the data within the tags is sensitive and should be transmitted via a secure channel.

Turning to FIG. **4**, illustrated is an example system **400** for providing a SSL/TLS encryption system that uses tags for multiple types of secure channels in accordance with one or more aspects of the disclosure. In an embodiment, a set of data **402** can include data **404** that does not require encryption, and can be sent via an unsecured channel. The set of data **402** can also include a first type of sensitive data **410** and a second set of sensitive data **416** that are identified by tags **406** and **408** and **412** and **414** respectively. The tags can identify the type of confidential data (e.g., S_1 , S_2) and can be transmitted via different secure channels based on one or more rules policies stored at the client or the server.

Turning now to FIG. **5**, illustrated is an example system **500** for providing a SSL/TLS encryption system that can identify sensitive information in accordance with one or more aspects of the disclosure.

In an embodiment, the sensitive data can be identified based on a pattern analysis of the data. Commonly transmitted data that might be sensitive and thus require encryption can be financial information such as bank account numbers, routing numbers, credit card numbers, and etc. The information can also include addresses, names, birthdates, and etc. These types of information commonly follow similar formats such as a pattern of numbers and characters, length of string of characters, and etc. For instance, social security numbers can be recognized by their familiar pattern of 9 numbers separated by dashes in groups of 3, 2, and 4. Similarly, credit card numbers will have common patterns and dates will have similar patterns and other identification numbers and information can be identified similarly.

In the embodiment shown in FIG. **5**, set of data can include unsecured data **504** and then include a social security number **506** and a telephone number **508**. The system can identify the social security number **506** based on the groupings of 3 digits, 2 digits, and 4 digits respectively separated by dashes. Similarly the phone number **508** can be identified in a similar fashion.

Turning now to FIG. **6**, illustrated is an example system **600** for providing a SSL/TLS encryption system **602** in accordance with one or more aspects of the disclosure. The system **602** can include an identification component **608** that can identify whether data to be transmitted is sensitive or not. Identification component **608** can determine what is sensitive data or data that otherwise should be encrypted in a variety of ways. In one embodiment, data can be tagged using metadata or HTML tags or other forms of tags, where the tagged data is data the intended to be secured via SSL encryption. In an embodiment, the identification component

608 can identify the tags, and communications component **604** can send untagged data via an unsecured channel and send tagged data via a secured channel.

In other embodiments, the sensitive data can be identified without the use of tags. Data that is static (e.g., the form templates, styles, outlines, etc) can be determined to be unsensitive and thus can be sent via the unsecured channel. Data that is dynamic, and changes between frames, sessions, etc, can be determined to be sensitive, and thus can be sent via the secured channel.

In other embodiments, the sensitive data can be identified based on a pattern analysis of the data. Commonly transmitted data that might be sensitive and thus require encryption can be financial information such as bank account numbers, routing numbers, credit card numbers, and etc. The information can also include addresses, names, birthdates, and etc. These types of information commonly follow similar formats such as a pattern of numbers and characters, length of string of characters, and etc. For instance, social security numbers can be recognized by their familiar pattern of 9 numbers separated by dashes in groups of 3, 2, and 4. Similarly, credit card numbers will have common patterns and dates will have similar patterns and other identification numbers and information can be identified similarly.

The communications component **604** can be configured to transmit the data to the server, or to a client device, and can simultaneously establish a plurality of communication channels, unsecured and secured. In an embodiment, the communications component **604** can establish two channels, one secured, and one unsecured, and in other embodiments, can establish one unsecured and a plurality of secured channels. Policy database **610** can determine how various types of data are to be treated and handled based on the type of data and the rules. For instance, in an embodiment, all sensitive data can be sent via a first secured channel, and in other embodiments, different types of sensitive data can be sent via different secured channels. An update component **606** can be included to update the policy database **610** based on information received from one or more servers.

FIGS. **7-8** illustrates processes in connection with the aforementioned systems. The process in FIGS. **7-8** can be implemented for example by systems **100**, **200**, **300**, **400**, **500**, and **600** illustrated in FIGS. **1-6** respectively. While for purposes of simplicity of explanation, the methods are shown and described as a series of blocks, it is to be understood and appreciated that the claimed subject matter is not limited by the order of the blocks, as some blocks may occur in different orders and/or concurrently with other blocks from what is depicted and described herein. Moreover, not all illustrated blocks may be required to implement the methods described hereinafter.

Turning now to FIG. **7**, illustrated is an example flow chart of a method **700** for providing encryption according to one or more embodiments.

The method can start at **702**, where the method includes establishing, by a mobile device comprising a processor, a plurality of data transmission channels to a server, wherein the data transmission channels are configured to transmit a set of data to the server and wherein the plurality of data transmission channels comprise an unsecured channel a secured channel.

The method can continue at **704**, where the method includes determining, by the mobile device, that the set of data comprises a first set of confidential data, and a second set of non-confidential data wherein the non-confidential data comprises static information and the confidential data comprises dynamic information. The method can continue at

706 where the method includes transmitting, by the mobile device, the first set of confidential data via the secured channel, and transmitting the non-confidential data via the unsecured channel.

Turning now to FIG. 8, illustrated is an example flow chart of a method 800 for providing encryption according to one or more embodiments.

Method 800 can start at 802 where the method includes transmitting, by the mobile device, the first subset of data in a first type of secured channel and transmitting the second subset of data in a second type of secured channel.

The method can continue at 804 where the method includes determining, by the mobile device, a type of secured channel to transmit the first subset of data and the second subset of data based on a security policy, wherein the security policy specifies rules about types of confidential data.

Referring now to FIG. 9, there is illustrated a block diagram of a computer operable to execute the disclosed architecture. In order to provide additional context for various aspects of the subject innovation, FIG. 9 and the following discussion are intended to provide a brief, general description of a suitable computing environment 900 in which the various aspects of the innovation can be implemented. While the innovation has been described above in the general context of computer-executable instructions that may run on one or more computers, those skilled in the art will recognize that the innovation also can be implemented in combination with other program modules or components and/or as a combination of hardware and software.

Generally, program modules include routines, programs, components, data structures, etc., that perform particular tasks or implement particular abstract data types. Moreover, the inventive methods can be practiced with other computer system configurations, including single-processor or multi-processor computer systems, minicomputers, mainframe computers, as well as personal computers, hand-held computing devices, microprocessor-based or programmable consumer electronics, and the like, each of which can be operatively coupled to one or more associated devices.

The illustrated aspects of the innovation may also be practiced in distributed computing environments where certain tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules can be located in both local and remote memory storage devices.

A computer typically includes a variety of computer-readable media. Computer-readable media can be any available media that can be accessed by the computer and includes both volatile and nonvolatile media, removable and non-removable media. By way of example, and not limitation, computer-readable media can comprise computer storage media and communication media. Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer-readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disk (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by the computer.

Communication media typically embodies computer-readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave

or other transport mechanism, and includes any information delivery media. The term “modulated data signal” means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer-readable media.

With reference again to FIG. 9, the exemplary environment 900 for implementing various aspects of the innovation includes a computer 902, the computer 902 including a processing unit 904, a system memory 906 and a system bus 908. The system bus 908 couples system components including, but not limited to, the system memory 906 to the processing unit 904. The processing unit 904 can be any of various commercially available processors. Dual microprocessors and other multi-processor architectures may also be employed as the processing unit 904.

The system bus 908 can be any of several types of bus structure that may further interconnect to a memory bus (with or without a memory controller), a peripheral bus, and a local bus using any of a variety of commercially available bus architectures. The system memory 906 includes read-only memory (ROM) 910 and random access memory (RAM) 912. A basic input/output system (BIOS) is stored in a non-volatile memory 910 such as ROM, EPROM, EEPROM, which BIOS contains the basic routines that help to transfer information between elements within the computer 902, such as during start-up. The RAM 912 can also include a high-speed RAM such as static RAM for caching data.

The computer 902 further includes an internal hard disk drive (HDD) 914 (e.g., EIDE, SATA), which internal hard disk drive 914 may also be configured for external use in a suitable chassis (not shown), a magnetic floppy disk drive (FDD) 916, (e.g., to read from or write to a removable diskette 918) and an optical disk drive 920, (e.g., reading a CD-ROM disk 922 or, to read from or write to other high capacity optical media such as the DVD). The hard disk drive 914, magnetic disk drive 916 and optical disk drive 920 can be connected to the system bus 908 by a hard disk drive interface 924, a magnetic disk drive interface 926 and an optical drive interface 928, respectively. The interface 924 for external drive implementations includes at least one or both of Universal Serial Bus (USB) and IEEE 1394 interface technologies. Other external drive connection technologies are within contemplation of the subject innovation.

The drives and their associated computer-readable media provide nonvolatile storage of data, data structures, computer-executable instructions, and so forth. For the computer 902, the drives and media accommodate the storage of any data in a suitable digital format. Although the description of computer-readable media above refers to a HDD, a removable magnetic diskette, and a removable optical media such as a CD or DVD, other types of media which are readable by a computer, such as zip drives, magnetic cassettes, flash memory cards, cartridges, and the like, may also be used in the exemplary operating environment, and further, that any such media may contain computer-executable instructions for performing the methods of the innovation.

A number of program modules can be stored in the drives and RAM 912, including an operating system 930, one or more application programs 932, other program modules 934 and program data 936. All or portions of the operating system, applications, modules, and/or data can also be

cached in the RAM 912. The innovation can be implemented with various commercially available operating systems or combinations of operating systems.

A user can enter commands and information into the computer 902 through one or more wired/wireless input devices, e.g., a keyboard 938 and a pointing device, such as a mouse 940. Other input devices (not shown) may include a microphone, an IR remote control, a joystick, a game pad, a stylus pen, touch screen, or the like. These and other input devices are often connected to the processing unit 904 through an input device interface 942 that is coupled to the system bus 908, but can be connected by other interfaces, such as a parallel port, an IEEE 1394 serial port, a game port, a USB port, an IR interface, etc.

A monitor 944 or other type of display device is also connected to the system bus 908 via an interface, such as a video adapter 946. In addition to the monitor 944, a computer typically includes other peripheral output devices (not shown), such as speakers, printers, etc.

The computer 902 may operate in a networked environment using logical connections via wired and/or wireless communications to one or more remote computers, such as a remote computer(s) 948. The remote computer(s) 948 can be a workstation, a server computer, a router, a personal computer, portable computer, microprocessor-based entertainment appliance, a peer device or other common network node, and typically includes many or all of the elements described relative to the computer 902, although, for purposes of brevity, only a memory/storage device 950 is illustrated. The logical connections depicted include wired/wireless connectivity to a local area network (LAN) 952 and/or larger networks, e.g., a wide area network (WAN) 954. Such LAN and WAN networking environments are commonplace in offices and companies, and facilitate enterprise-wide computer networks, such as intranets, all of which may connect to a global communications network, e.g., the Internet.

When used in a LAN networking environment, the computer 902 is connected to the local network 952 through a wired and/or wireless communication network interface or adapter 956. The adapter 956 may facilitate wired or wireless communication to the LAN 952, which may also include a wireless access point disposed thereon for communicating with the wireless adapter 956.

When used in a WAN networking environment, the computer 902 can include a modem 958, or is connected to a communications server on the WAN 954, or has other means for establishing communications over the WAN 954, such as by way of the Internet. The modem 958, which can be internal or external and a wired or wireless device, is connected to the system bus 908 via the serial port interface 942. In a networked environment, program modules or components depicted relative to the computer 902, or portions thereof, can be stored in the remote memory/storage device 950. The network connections shown are exemplary and other means of establishing a communications link between the computers can be used.

The computer 902 is operable to communicate with any wireless devices or entities operatively disposed in wireless communication, e.g., a printer, scanner, desktop and/or portable computer, portable data assistant, communications satellite, any piece of equipment or location associated with a wirelessly detectable tag (e.g., a kiosk, news stand, restroom), and telephone. This includes at least Wi-Fi and Bluetooth™ wireless technologies. Thus, the communica-

tion can be a predefined structure as with a conventional network or simply an ad hoc communication between at least two devices.

Wi-Fi, or Wireless Fidelity, allows connection to the Internet from a couch at home, a bed in a hotel room, or a conference room at work, without wires. Wi-Fi is a wireless technology similar to that used in a cell phone that enables such devices, e.g., computers, to send and receive data indoors and out; anywhere within the range of a base station. Wi-Fi networks use radio technologies called IEEE 802.11 (a, b, g, n, etc.) to provide secure, reliable, fast wireless connectivity. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wired networks (which use IEEE 802.3 or Ethernet). Wi-Fi networks operate in the unlicensed 2.4 and 5 GHz radio bands, at an 11 Mbps (802.11a) or 54 Mbps (802.11b) data rate, for example, or with products that contain both bands (dual band), so the networks can provide real-world performance similar to wired Ethernet networks used in many offices.

Referring now to FIG. 10, there is illustrated a schematic block diagram of an exemplary computing environment 1000 in accordance with the subject innovation. The system 1000 includes one or more client(s) 1002. The client(s) 1002 can be hardware and/or software (e.g., threads, processes, computing devices).

The system 1000 also includes one or more server(s) 1004. The server(s) 1004 can also be hardware and/or software (e.g., threads, processes, computing devices). The servers 1004 can house threads to perform transformations by employing the innovation, for example. One possible communication between a client 1002 and a server 1004 can be in the form of a data packet adapted to be transmitted between two or more computer processes. The system 1000 includes a communication framework 1006 (e.g., a global communication network such as the Internet) that can be employed to facilitate communications between the client(s) 1002 and the server(s) 1004.

Communications can be facilitated via a wired (including optical fiber) and/or wireless technology. The client(s) 1002 are operatively connected to one or more client data store(s) 1008 that can be employed to store information local to the client(s) 1002. Similarly, the server(s) 1004 are operatively connected to one or more server data store(s) 1010 that can be employed to store information local to the servers 1004.

What has been described above includes examples of the innovation. It is, of course, not possible to describe every conceivable combination of components or methodologies for purposes of describing the subject innovation, but one of ordinary skill in the art may recognize that many further combinations and permutations of the innovation are possible. Accordingly, the innovation is intended to embrace all such alterations, modifications and variations that fall within the spirit and scope of the appended claims. Furthermore, to the extent that the term “includes” is used in either the detailed description or the claims, such term is intended to be inclusive in a manner similar to the term “comprising” as “comprising” is interpreted when employed as a transitional word in a claim.

The invention claimed is:

1. A system, comprising:
 - a memory configured to store computer-executable instructions; and
 - a processor, communicatively coupled to the memory, configured to execute the computer-executable instructions to perform operations, the operations comprising: establishing a plurality of data transmission channels to a server, wherein the plurality of data transmission

13

channels are configured to transmit a set of data to the server and wherein the plurality of data transmission channels comprise at least an unsecured channel and a plurality of secured channels, wherein a type of the a secured channel of the plurality of secured channels is established based at least on a time or location of the transmission of the set of data to the server;

determining that the set of data comprises a first set of confidential data, and a second set of non-confidential data, wherein the system differentiates between confidential and non-confidential data via the use of tags on a page or frame, and wherein tags are used to determine a security policy used, wherein the non-confidential data comprise static information and the confidential data comprise dynamic information, the dynamic information changing between frames or sessions; and transmitting the first set of confidential data via the plurality of secured channels, and transmitting the non-confidential data via the unsecured channel, wherein the first set of confidential data comprises a first subset of a first type of confidential data and a second subset of a second type of confidential data, wherein the plurality of secured channels may be opened simultaneously between the server and a mobile device in order to allow for the transmittal of different types of confidential data simultaneously.

2. The system of claim 1, wherein determining further comprises identifying a tag that identifies the first set of confidential data.

3. The system of claim 2, wherein the tag indicates the type of confidential data that the first set of confidential data is associated with.

4. The system of claim 1, wherein the operations further comprise:

transmitting the first subset of data in a first type of secured channel of the plurality of secured channels and transmitting the second subset of data in a second type of secured channel of the plurality of secured channels.

5. The system of claim 4, wherein the operations further comprise:

determining a type of secured channel of the plurality of secured channels to transmit the first subset of data and the second subset of data based on a security policy, wherein the security policy specifies a first set of rules for determining types of secured channels of the plurality of secured channels and a second set of rules about types of confidential data.

6. The system of claim 5, wherein the first and second sets of rules specify which types of encryption are used for respective types of confidential data and who is authorized to access the confidential data.

7. The system of claim 1, wherein the non-confidential data comprise page layout information, style information, and template information, and the confidential data comprise name information, address information, financial information and other identifying information.

8. The system of claim 1, wherein determining further comprises identifying the first set of confidential data by matching a data sequence to a predetermined sequence, wherein the data sequence comprises at least one of character type, character length, and character sequence.

9. The system of claim 1 further comprising:

a mobile device that realizes improved battery life based at least in part on the reduced computing resources of

14

the established plurality of data transmission channels and the transmitting of the first set of confidential data via the plurality of secured channels, and the transmitting of the non-confidential data via the unsecured channel.

10. The system of claim 1, wherein determining that the set of data comprises a first set of confidential data is based on pattern analysis.

11. A method for providing secured communications, comprising:

establishing, by a mobile device comprising a processor, a plurality of data transmission channels to a server, wherein the plurality of data transmission channels are configured to transmit a set of data to the server and wherein the plurality of data transmission channels comprise at least an unsecured channel and a plurality of secured channels, wherein a type of a secured channel of the plurality of secured channels is established based at least on a time or location of the transmission of the set of data to the server;

determining, by the mobile device, that the set of data comprises a first set of confidential data, and a second set of non-confidential data wherein the non-confidential data comprise static information and the confidential data comprise dynamic information, the dynamic information changing between frames or sessions, wherein the processor differentiates between confidential and non-confidential data via the use of tags on a page or frame, and wherein tags are used to determine a security policy used; and transmitting, by the mobile device, the first set of confidential data via the plurality of secured channels, and transmitting the non-confidential data via the unsecured channel wherein the first set of confidential data comprises a first subset of a first type of confidential data and a second subset of a second type of confidential data, wherein the plurality of secured channels may be opened simultaneously between the server and a mobile device in order to allow for the transmittal of different types of confidential data simultaneously.

12. The method of claim 11, wherein determining that the set of data comprises the first set of confidential data is based on identifying a tag that identifies the first set of confidential data.

13. The method of claim 12, wherein the tag indicates the type of confidential data that the first set of confidential data is associated with.

14. The method of claim 11, further comprising:

transmitting, by the mobile device, the first subset of data in a first type of secured channel of the plurality of secured channels and transmitting the second subset of data in a second type of secured channel of the plurality of secured channels.

15. The method of claim 14, further comprising:

determining, by the mobile device, a type of secured channel of the plurality of secured channels to transmit the first subset of data and the second subset of data based on a security policy, wherein the security policy specifies a first set of rules for determining types of secured channels of the plurality of secured channels and a second set of rules about types of confidential data.

16. The method of claim 15, wherein the first and second sets of rules specify which types of encryption are used for respective types of confidential data and who is authorized to access the confidential data.

15

17. The method of claim 11, wherein determining further comprises identifying the first set of confidential data by matching a data sequence to a predetermined sequence, wherein the data sequence comprises at least one of character type, character length, and character sequence. 5

18. The method of claim 11, wherein determining that the set of data comprises a first set of confidential data is based on pattern analysis.

19. A non-transitory computer-readable medium, comprising instructions that when executed by a computer processor perform operations, comprising: 10

establishing a plurality of data transmission channels to a server, wherein the plurality of data transmission channels are configured to transmit a set of data to the server and wherein the plurality of data transmission channels comprise an unsecured channel and a plurality of secured channels, wherein a type of a secured channel of the plurality of secured channels is established based at least on a time or location of the transmission of the set of data to the server; 15

determining that the set of data comprises a first set of confidential data, and a second set of non-confidential data, wherein the system differentiates between confidential and non-confidential data via the use of tags on a page or frame, and wherein tags are used to determine a security policy used, 25

wherein the non-confidential data comprise static information and the confidential data comprise dynamic

16

information, the dynamic information changing between frames or sessions, and

further wherein the first set of confidential data comprises a first subset of a first type of confidential data and a second subset of a second type of confidential data; and

transmitting the first set of confidential data via the plurality of secured channels, and transmitting the non-confidential data via the unsecured channel, wherein the plurality of secured data channels utilize different types of encryption based on the type of data being transmitted.

20. The non-transitory computer-readable medium of claim 19, wherein the operations further comprise:

transmitting the first subset of data in a first type of secured channel of the plurality of secured channels and transmitting the second subset of data in a second type of secured channel of the plurality of secured channels; and

determining, by the mobile device, a type of secured channel of the plurality of secured channels to transmit the first subset of data and the second subset of data based on a security policy, wherein the security policy specifies a first set of rules for determining types of secured channels of the plurality of secured channels and a second set of rules about types of confidential data.

* * * * *